

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 10-285157
(43)Date of publication of application : 23.10.1998

(51)Int.Cl. H04L 9/32
G09C 1/00
H04L 9/08

(21)Application number : 09-092437 (71)Applicant : NIPPON TELEGR & TELEPH CORP

(22) Date of filing : 10.04.1997 (72) Inventor : HASHIMOTO SHOICHI
MORI MASAAKI
NAKAHARA SHINICHI

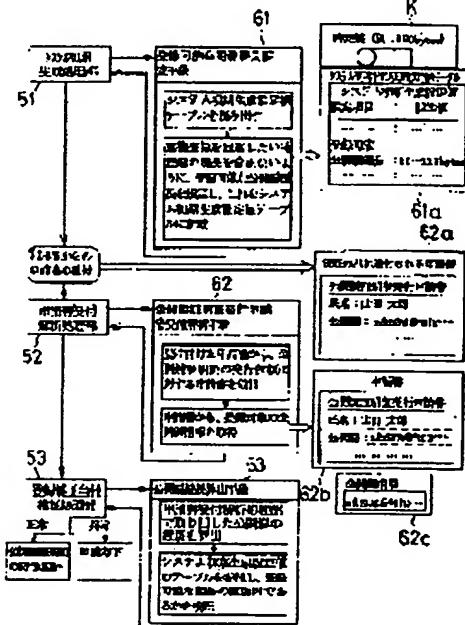
REST AVAILABLE COPY

54) REGISTRATION KEY DUPLEX PREVENTING DEVICE IN AUTHENTICATION SYSTEM

(57) Abstract:

PROBLEM TO BE SOLVED: To recognize whether an applied open key is justly generated or not and to prevent the duplex of a registration key by receiving application information where an electronic signature is given by a secret key, extracting filled open key information, certifying it with the electronic signature and recognizing the validity or invalidity of application.

SOLUTION: An open key length calculation means 63 is called for recognizing whether open key information 62c filled in an application open key certificate issuing application 62a is valid application or not in a registration key validity verification processing part 53. The key length of the open key obtained in an application reception analysis processing part 52 is calculated and whether it is within the range of a registration possible open key length which is set in a system initial generation processing part 51 or not is verified. When verification justly terminates, the issuing processing of the open key certificate is executed by setting application to be just. Since the open key in length different from specified key length is registered, the registration of the open key duplexed with the open key is avoided. Even if the user imitates and applies the specified open key, the verification system easily recognizes it and rejects application.



LEGAL STATUS

[Date of request for examination] 01.02.2001

[Date of sending the examiner's decision of rejection] 18.05.2004

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

(51) Int.Cl.^{*}
 H 04 L 9/32
 G 09 C 1/00
 H 04 L 9/08

識別記号
 6 4 0

F I
 H 04 L 9/00
 G 09 C 1/00
 H 04 L 9/00

6 7 5 D
 6 4 0 B
 6 0 1 F

審査請求 未請求 請求項の数2 OL (全9頁)

(21) 出願番号 特願平9-92437
 (22) 出願日 平成9年(1997)4月10日

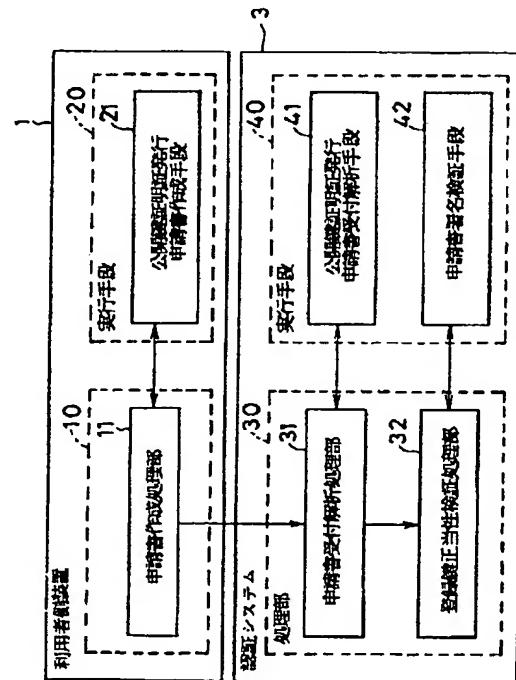
(71) 出願人 000004226
 日本電信電話株式会社
 東京都新宿区西新宿三丁目19番2号
 (71) 出願人 000102717
 エヌ・ティ・ティ・ソフトウェア株式会社
 神奈川県横浜市中区山下町223番1
 (72) 発明者 橋本 正一
 東京都新宿区西新宿三丁目19番2号 日本
 電信電話株式会社内
 (72) 発明者 森 正昭
 東京都新宿区西新宿三丁目19番2号 日本
 電信電話株式会社内
 (74) 代理人 井理士 三好 秀和 (外1名)
 最終頁に続く

(54)【発明の名称】認証システムにおける登録鍵重複防止装置

(57)【要約】

【課題】 本発明は、利用者が公開鍵の登録申請を行う際に、登録対象の公開鍵が申請者自身によって正当に生成されたものであることを、認証システムが短時間で簡単に確認することを可能とする認証システムにおける登録鍵重複防止装置を提供することを目的とする。

【解決手段】 登録する公開鍵を含み、かつ当該公開鍵に対応する秘密鍵を用いて電子署名を施した申請情報を受け付け、当該申請書内に記載されている公開鍵情報を抽出する申請書内公開鍵情報取得手段と、この申請書内公開鍵情報取得手段で抽出された公開鍵によって、前記申請書に付与された電子署名を検証し、検証が正常なときを正当な申請、異常なときを不当な申請とする申請書署名検証手段とを備えて構成される。



【特許請求の範囲】

【請求項1】 特定される公開鍵の持ち主であることを証明する公開鍵証明証を発行する公開鍵暗号方式を用いた認証システムにおける登録鍵重複防止装置であって、登録する公開鍵を含み、かつ当該公開鍵に対応する秘密鍵を用いて電子署名を施した申請情報を受け付け、当該申請書内に記載されている公開鍵情報を抽出する申請書内公開鍵情報取得手段と、この申請書内公開鍵情報取得手段で抽出された公開鍵情報によって、前記申請書に付与された電子署名を検証し、検証が正常なときを正当な申請、異常なときを不当な申請とする申請書署名検証手段とを有することを特徴とする認証システムにおける登録鍵重複防止装置。

【請求項2】 特定される公開鍵の持ち主であることを証明する公開鍵証明証を発行する公開鍵暗号方式を用いた認証システムにおける登録鍵重複防止装置であって、利用者からの公開鍵証明証の発行申請書を受け付け、当該発行申請書内に記載されている公開鍵情報を抜き出す申請書内公開鍵情報取得手段と、

この申請書内公開鍵情報取得手段で抜き出された公開鍵の鍵長を算出し、重複を回避したい特定の鍵の鍵長とは異なる鍵長の鍵のみを正当な申請とみなす公開鍵鍵長算出手段とを有することを特徴とする認証システムにおける登録鍵重複防止装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 本発明は、公開鍵暗号方式で利用される公開鍵の正当性を証明する認証システムにおける登録鍵重複防止装置に関するものである。

【0002】

【従来の技術】 コンピュータネットワーク上で電子データ交換（EDI : Electronic Data Interchange）や電子商取引（EC : Electronic Commerce）を実現する際には、盗聴／なりすまし／改ざん／送信否認などの脅威が想定される。そのため、これら脅威からシステムを防御するために、一般的に暗号通信やディジタル署名通信が用いられる。この暗号方式は、例えば参考文献「Diffie, W. and Hellman, M. : New Directions in Cryptography, IEEE Trans. Inf. Theory, IT-22, 6 pp. 644-654, 1976」で発表されており、世の中で広く知られるところとなっている。

【0003】 このような公開鍵暗号方式では、一般に広く公開しておく公開鍵と、自分のみが知り得る秘密鍵の2種類の鍵を用いて通信が行われる。ここで、公開鍵を単に周知するだけでは他人を装って周知する「なりすまし」と呼ばれる脅威が考えられることから、公開鍵の正当な持ち主であることを証明する第三者機関が必要であり、それが認証局（CA : Certification Authority）と呼ばれるものである。

【0004】 この認証局を含む認証システムは、コンピ

ュータネットワーク上で取引関係にある企業間での取引を電子交換する電子データ交換やコンピュータネットワーク上で情報を伝達、処理し電子決済等の商取引を行う電子商取引を実現する際に、送信データの秘匿性や改ざん防止の目的で利用される公開鍵暗号方式に関して、その公開鍵証明証を発行／管理するシステムである。すなわち、認証システムは、日本の実社会で、実印の持ち主を証明する印鑑証明書を役所が発行するのと同様に、デジタル通信の世界で、公開鍵の持ち主を証明する公開鍵証明証を発行する機能を持ったシステムであるということができる。

【0005】 一般的に認証システムの機能として、次の4つが知られている。

- (1) 公開鍵登録機能…利用者が申請した公開鍵に対して、公開鍵証明証を作成／登録／発行する。
- (2) 証明証参照機能…認証システムで管理している公開鍵証明証を利用者から参照可能とする。
- (3) 公開鍵無効化機能…公開鍵証明証を無効化し、無効化リストに掲載する。
- (4) 無効化リスト参照機能…無効化された公開鍵証明証の一覧を利用者から参照可能とする。

【0006】 これらの機能は、コンピュータシステムや暗号アルゴリズムにより既に提供されている一般的な手段を用いて構築可能であり、申請時に申請書を用いた依頼を行うこと、認証システムと利用者の間ではデジタル署名通信を行うこと、公開鍵証明証や無効化リストをディレクトリやデータベースに管理しておくこと、などの基本的な構成方式についても、既に一般的方法であると認知されている。

【0007】 さて、利用者が認証システムに対して公開鍵証明証の発行を依頼する場合、利用者は、登録したい公開鍵の情報を認証システムに提示し、認証システムはこの受け付けた公開鍵情報に対して証明証を発行するという手順を踏むことになる。ここで、認証システムに対して提示する公開鍵情報は、既に公開されている情報である。そのため、例えば利用者が既に登録されている他の人の公開鍵情報を真似て、全く同一の鍵を公開鍵として認証システムに登録してしまう、すなわち利用者が自分で正当に作成していない公開鍵を認証システムに登録してしまう可能性が生じる。

【0008】 このようにして、既に登録済の公開鍵と同一の公開鍵の登録が行われた場合、複数の異なる利用者の公開鍵証明証の中に、同一の公開鍵情報が記載されている状況が生じることになる。これにより公開鍵証明証の利用者は、どちらが正当な公開鍵証明証であるのかが区別できず混乱を引き起こすことになる。また、認証システムの公開鍵のように、認証システムにおいて重要な特定の公開鍵に対して、上記のような問題が生じた場合には更に混乱を極めることになる。

【0009】 そこでこの問題を解決するための最も基本

的な方法として、申請者が登録を申請してきた公開鍵情報に対して、これと同一の公開鍵がすでに認証システムの管理する公開鍵証明証の中に存在するかどうかを検索して確認するという方法が考えられる。

【0010】

【発明が解決しようとする課題】しかしながら、上記の認証システムが管理する公開鍵証明証をすべて読み出して、この公開鍵証明証に記載されている公開鍵情報を参照して、申請された公開鍵と同一の公開鍵の有無を検索するという方法は、近い将来には公開鍵証明証の個数が膨大となることが予想されることから、読み出しと検索に多大な時間を要する上記方法は現実的では無い。

【0011】本発明は、上記課題に鑑みてなされたもので、利用者が公開鍵の登録申請を行う際に、登録対象の公開鍵が申請者自身によって正当に生成され、他人の公開鍵と同一のものではないことを、認証システムが短時間で簡易に確認して、不当な申請の場合にはこれを却下することを可能とする認証システムにおける登録鍵重複防止装置を提供することを目的とする。

【0012】

【課題を解決するための手段】前述した目的を達成するために、本発明の請求項1記載の発明は、特定される公開鍵の持ち主であることを証明する公開鍵証明証を発行する公開鍵暗号方式を用いた認証システムにおける登録鍵重複防止装置であって、登録する公開鍵を含み、かつ当該公開鍵に対応する秘密鍵を用いて電子署名を施した申請情報を受け付け、当該申請書内に記載されている公開鍵情報を抽出する申請書内公開鍵情報取得手段と、この申請書内公開鍵情報取得手段で抽出された公開鍵によって、前記申請書に付与された電子署名を検証し、検証が正常なときを正当な申請、異常なときを不当な申請とする申請書署名検証手段とを有することを要旨とする。

【0013】請求項1記載の本発明では、正当な申請者のみが持っている登録鍵（公開鍵）に対応する秘密鍵を用いて、申請者が公開鍵を登録する際の申請書に対して電子署名を作成し、これを申請書に付与して認証システムに送付し、これを受け付けた認証システムが、申請書に付与する電子署名を検証して正当な登録であることを確認することにより、申請された公開鍵が申請者によって正当に生成され、他の公開鍵を真似したものでないことを簡易に確認し、登録鍵の重複を防止できることに特徴がある。

【0014】また、本発明の請求項2記載の発明は、特定される公開鍵の持ち主であることを証明する公開鍵証明証を発行する公開鍵暗号方式を用いた認証システムにおける登録鍵重複防止装置であって、利用者からの公開鍵証明証の発行申請書を受け付け、当該発行申請書内に記載されている公開鍵情報を抜き出す申請書内公開鍵情報取得手段と、この申請書内公開鍵情報取得手段で抜き出された公開鍵の鍵長を算出し、重複を回避したい特定

の鍵の鍵長とは異なる鍵長の鍵のみを正当な申請とみなす公開鍵鍵長算出手段とを有することを要旨とする。

【0015】請求項2記載の本発明では、特定の鍵の鍵長と異なる鍵長を持つ公開鍵のみを登録可能な公開鍵として規定することにより、申請された公開鍵が特定の鍵と重複しないことを簡易に確認することができるに特徴がある。

【0016】

【発明の実施の形態】以下、図面を用いて本発明の実施の形態について説明する。図1は本発明の一実施の形態に係る認証システムの構成を示すブロック図である。図1において、利用者側装置1は処理部10とこの処理部10に対応して設けられる実行手段20により構成され、処理部10は申請書作成処理部11を含み、実行手段20には申請書作成処理部11に対応して公開鍵証明証発行申請書作成手段21が用意される。同様に、認証システム3は処理部30とこの処理部30に対応して設けられる実行手段40により構成され、処理部30は申請書受付解析処理部31と登録鍵正当性検証処理部32とを含み、実行手段40には申請書受付解析処理部31に対応して公開鍵証明証発行申請書受付解析手段41が、登録鍵正当性検証処理部32に対応して申請書署名検証手段42がそれぞれ用意される。

【0017】以下、図1乃至図3を参照して、各処理部における実行手段の作用を処理手順に従って説明する。まず、利用者側装置1の申請書作成処理部11において、ステップS1で、公開鍵証明証発行申請書作成手段21を用いて、登録する公開鍵情報を記述した公開鍵証明証発行申請書21aに対して、その公開鍵に対応する秘密鍵を用いて電子署名21bを作成し、これを申請書に付与した申請書21cを認証システム3に送付する。

【0018】一方、認証システム側の申請書受付解析処理部31において、ステップS2で、公開鍵証明証発行申請書受付解析手段41を用いて、利用者側装置1から送付された申請書から公開鍵証明証の発行依頼に係る申請書、すなわち公開鍵証明証発行申請書21cを受け付け、この公開鍵証明証発行申請書21cから申請情報部41a、電子署名部41bとを分離、抽出し、さらに申請情報部41aから公開鍵情報41cを取得する。

【0019】さらにステップS3では、登録鍵正当性検証処理部32において、申請書署名検証手段42を用いて、申請書に付与された電子署名を、申請書受付解析処理部31で取得した公開鍵を用いて、その正当性を検証する。この処理が正常に終了した場合には、申請者は申請者自身が正当に秘密鍵と公開鍵を生成し、このうちの公開鍵を登録申請してきたものとみなすことができるところから正当な登録であるとみなし、異常終了した場合には、申請者は登録申請した公開鍵に対応する秘密鍵を持っていないとみなすことができることから不当な登録であるとみなし、この公開鍵証明証の発行依頼に係る申請

では、システム初期生成値を管理するシステム初期生成設定値テーブル61aにおいて、登録可能公開鍵鍵長の項目を設け、ここに認証システム5が利用者からの重複登録を回避したい特定鍵の鍵長を含まない範囲の鍵長を、登録可能な鍵長として設定する。

【0032】ここで、システム初期生成値の管理は、一般的のコンピュータシステムにおいて提供されている機能を用いて容易に実現可能である。

【0033】次に、申請書受付解析処理部52における申請書受付解析処理について説明する。申請書受付解析処理部52では、公開鍵証明証発行申請書受付解析手段62を用いて、まず、利用者から送付されてきた公開鍵証明証の発行サービスに対する依頼申請書62aの受付を行う。そして次に、この公開鍵証明証発行申請書62aの解析処理として、サービス実行に必要となる情報を申請書から抜き出す処理を行う。ここでは、公開鍵証明証発行申請書62aから公開鍵情報62cを取得する。

【0034】尚、申請書の受信はコンピュータシステムが一般に提供している方法、例えば電子メールなどを用いて実現でき、申請書からの必要事項の取得も、同様に電子情報の読み取り機能などを用いて簡単に実現できる。

【0035】次に、登録鍵正当性検証処理部53における登録鍵正当性検証処理について説明する。登録鍵正当性検証処理部53では、申請書公開鍵証明証発行申請書62aに記載された公開鍵情報62cが、特定の鍵を真似たものでなく、正当な申請であるか否かを確認するために、公開鍵鍵長算出手段63を呼び出して、申請書受付解析処理部52で取得した公開鍵の鍵長を算出し、システム初期生成処理部51で設定した登録可能公開鍵鍵長の範囲内にあるかどうかを検証する。ここで検証が正当に終了した場合には、申請された公開鍵と特定鍵とは明らかに異なるものであることが確認され、申請が正当なものであるとみなし、公開鍵証明証の発行処理を行う。検証が異常に終了した場合には、申請された公開鍵が不当なものであるとみなし、申請を却下する。

【0036】尚、公開鍵の鍵長の算出は、一般にコンピュータシステムが提供するビット処理機能によって容易にかつ高速で実現可能である。

【0037】本実施形態によれば、特定の鍵の鍵長と異なる鍵長を持つ公開鍵のみが登録されることから、この特定の鍵と重複した公開鍵の登録を簡単に回避することができる。したがって、利用者が、特定の公開鍵を真似て申請してきた場合には、認証システムは簡単にこれを確認してこの申請を却下することが可能になる。

【0038】

【発明の効果】以上説明したように、本発明のうち請求項1記載の認証システムにおける登録鍵重複防止装置は、公開鍵に対応する秘密鍵を用いて電子署名を施した申請情報を受け付け、当該申請書内に記載されている公

開鍵情報を抽出し、この公開鍵情報によって、前記申請書に付与された電子署名を検証し、検証が正常なときを正当な申請、異常なときを不当な申請とするようにしたので、申請された公開鍵が申請者によって正当に生成され、他人の公開鍵を真似たものでないことを簡易に確認し、登録鍵の重複を防止できる等の効果を奏する。

【0039】また、本発明のうち請求項2記載の認証システムにおける登録鍵重複防止装置は、公開鍵証明証の発行申請書内に記載されている公開鍵情報を抜き出し、この公開鍵の鍵長を算出し、重複を回避したい特定の鍵の鍵長とは異なる鍵長の鍵のみを正当な申請とみなすようにしたので、申請された公開鍵が特定の鍵と重複しないことを簡易に確認することができる等の効果を奏する。

【0040】上述したように、本発明によれば利用者が公開鍵を登録申請を認証システムに対して行った際に、申請された公開鍵が、利用者自身で正当に生成した公開鍵でなく、既に登録済の公開鍵を真似て申請するというような不当な申請であるか否かを、短時間で簡易に確認できる登録鍵重複防止方法を構築することが可能になる。この方法を利用することによって、認証システムにおける登録鍵重複防止サービスを提供することが可能になる。

【図面の簡単な説明】

【図1】本発明に係る登録鍵重複防止装置が適用される認証システムの一実施の形態の概略の構成を示すブロック図である。

【図2】図1に示した認証システムにおける登録鍵重複防止装置の利用者側における処理を説明するためのブロック図である。

【図3】図1に示した認証システムにおける登録鍵重複防止装置の認証システム側における処理を説明するためのブロック図である。

【図4】本発明に係る登録鍵重複防止装置が適用される認証システムの他の実施の形態の概略の構成を示すブロック図である。

【図5】図4に示した登録鍵重複防止装置における処理を説明するためのブロック図である。

【符号の説明】

- 1 利用者側装置
- 3, 5 認証システム
- 10, 30, 50 処理部
- 11 申請書作成処理部
- 20, 40, 60 実行手段
- 21 公開鍵証明証発行申請書作成手段
- 21a 公開鍵証明証発行申請書
- 21b 申請書の電子署名
- 21c 認証システムに送付する申請書
- 31 申請書受付解析処理部
- 32 登録鍵正当性検証処理部

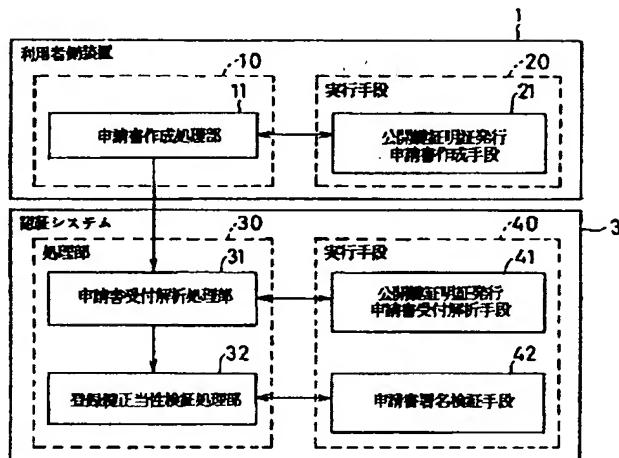
9

4 1 公開鍵証明証発行申請書受付解析手段
 4 1 a 申請情報部
 4 1 b 電子署名部
 4 1 c 公開鍵情報
 4 2 申請書署名検証手段
 5 1 システム初期生成処理部
 5 2 申請書受付解析処理部

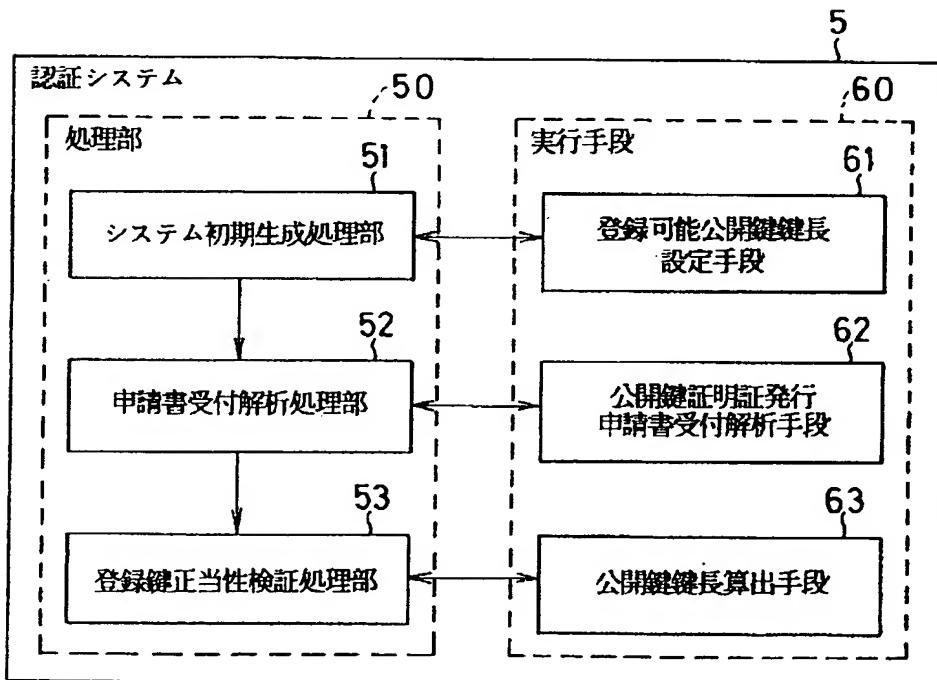
10

5 3 登録鍵正当性検証処理部
 6 1 登録可能公開鍵鍵長設定手段
 6 1 a システム初期生成設定値テーブル
 6 2 公開鍵証明証発行申請書受付解析手段
 6 2 a 申請書
 6 3 公開鍵鍵長算出手段

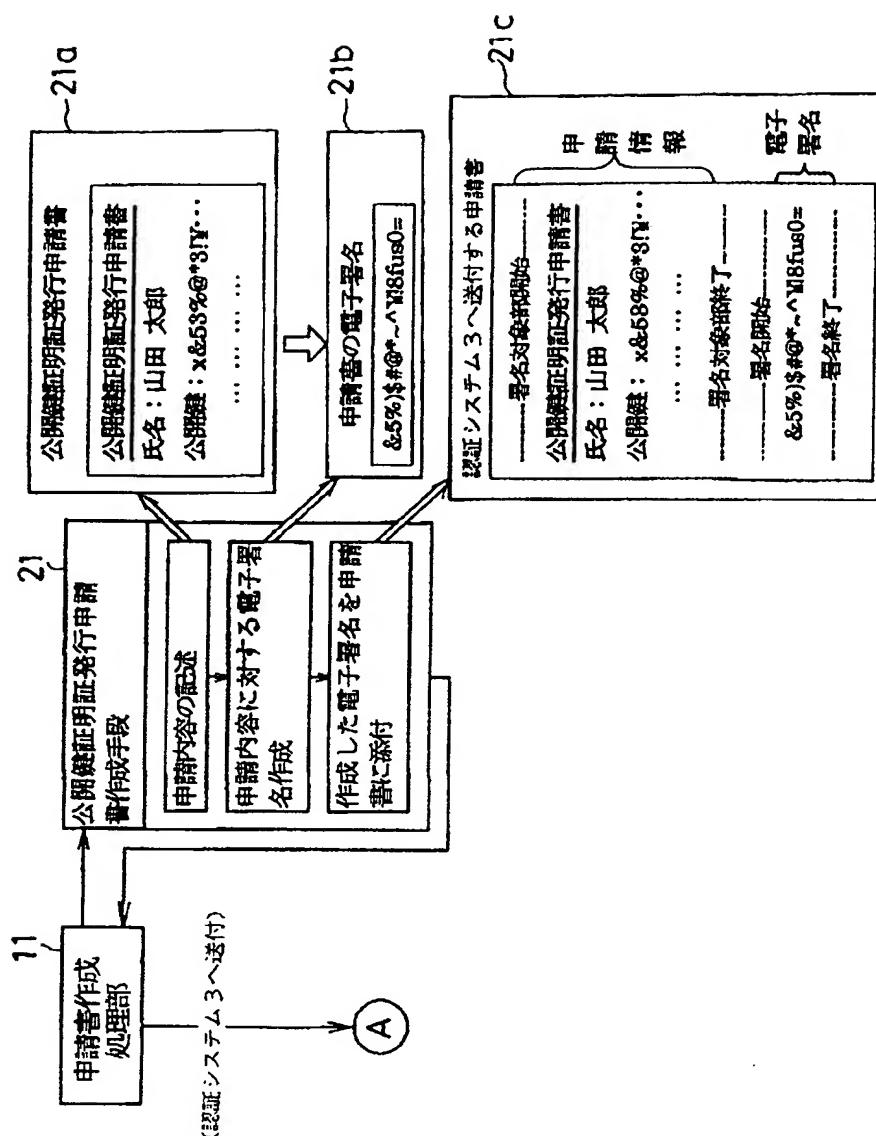
【図1】



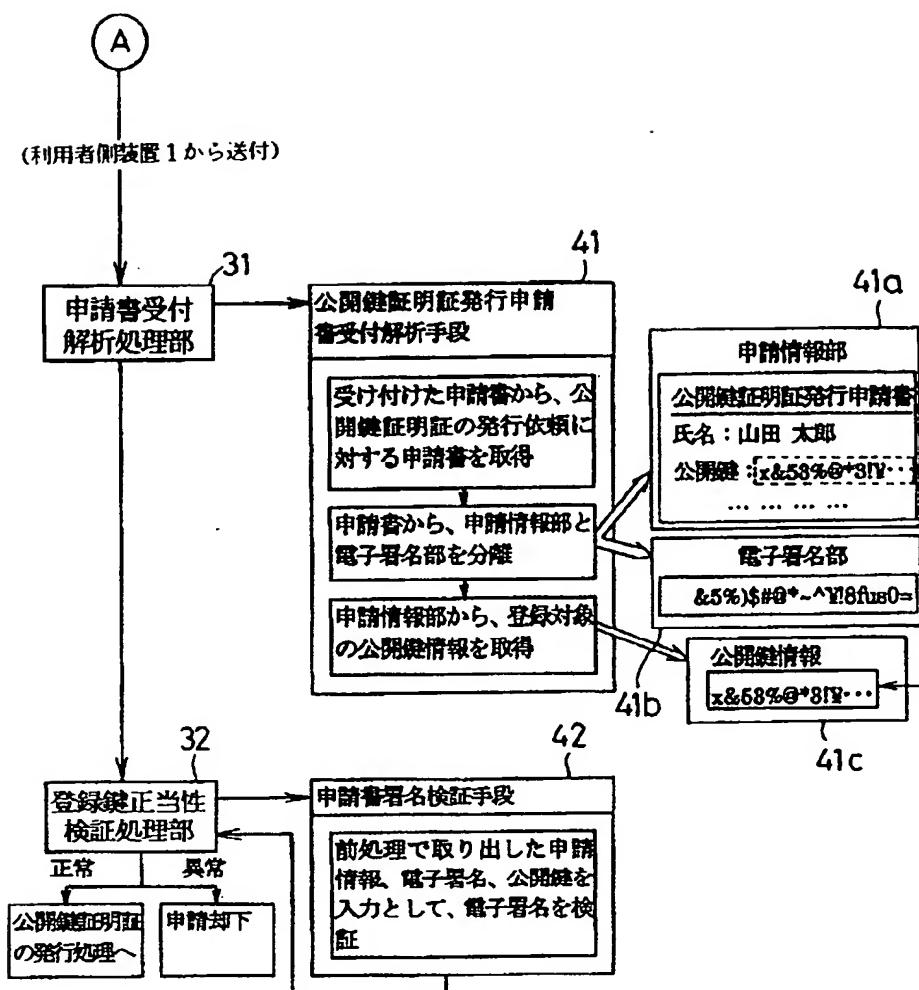
【図4】



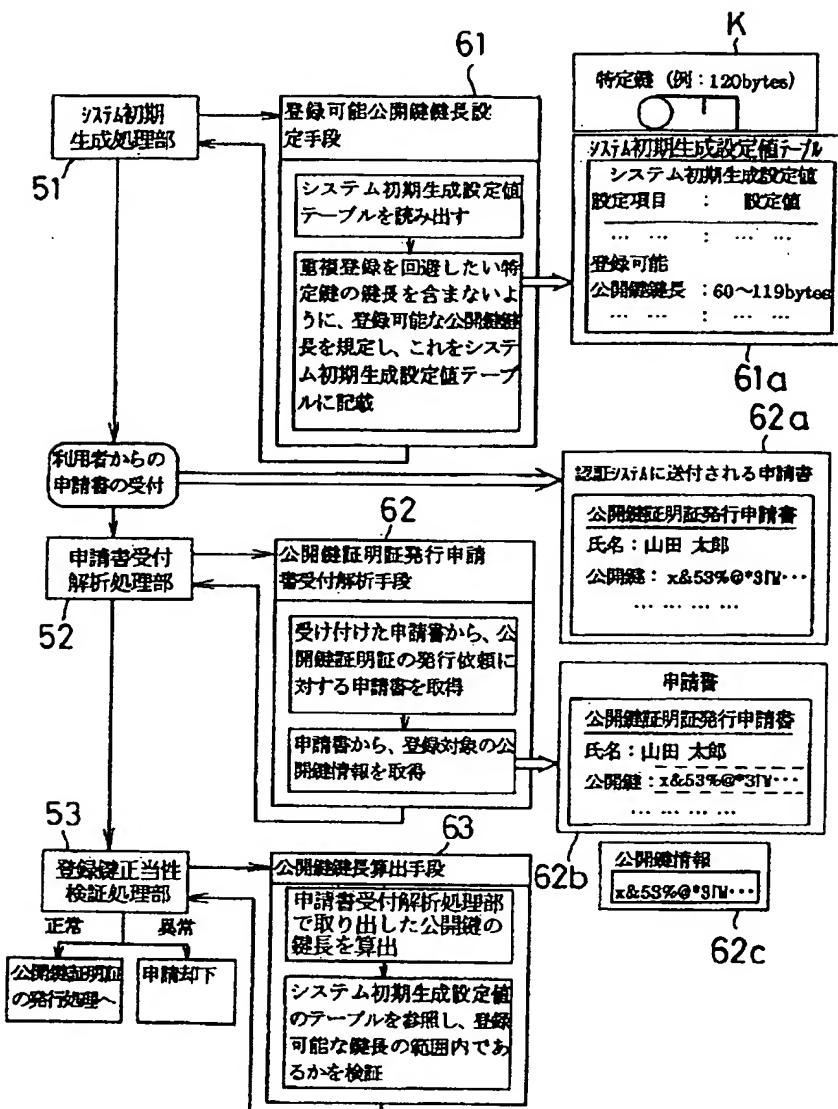
【図2】



【図3】



【図5】



フロントページの続き

(72)発明者 中原 慎一

神奈川県横浜市中区山下町223番1 エ

ヌ・ティ・ティ・ソフトウェア株式会社内

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- BLACK BORDERS**
- IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- FADED TEXT OR DRAWING**
- BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- SKEWED/SLANTED IMAGES**
- COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- GRAY SCALE DOCUMENTS**
- LINES OR MARKS ON ORIGINAL DOCUMENT**
- REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- OTHER: _____**

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.